

PATENTS

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

**Applicant:** TOMIHIKO AZUMA

**Docket:** 14739

**Serial No:** Unassigned

**Dated:** July 2, 2001

**Filed:** Herewith

**For: SECURE MAIL PROXY SYSTEM, METHOD OF  
MANAGING SECURITY, AND RECORDING MEDIUM**


Assistant Commissioner for Patents  
United States Patent and Trademark Office  
Washington, D.C. 20231

**CLAIM OF PRIORITY**

Sir:

Applicant in the above-identified application hereby claims the right of  
priority in connection with Title 35 U.S.C. § 119 and in support thereof, herewith submits  
a certified copy of Japanese Patent Application No. 2000-204112, filed on July 5, 2000.

Respectfully submitted,

  
Paul J. Esatto, Jr.  
Registration No. 30,749

Scully, Scott, Murphy & Presser  
400 Garden City Plaza  
Garden City, New York 11530  
(516) 742-4343

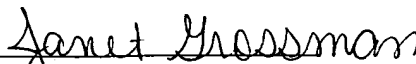
---

**CERTIFICATE OF MAILING BY "EXPRESS MAIL"**

**"Express Mail" Mailing Label Number: EL-894-227-674-US**  
**Date of Deposit: July 2, 2001.**

I hereby certify that this correspondence is being deposited with the United States Postal  
Service "Express Mail Post Office to Addressee" service under 37 C.F.R. § 1.10 on the date  
indicated above and is addressed to the Assistant Commissioner for Patents and Trademarks,  
Washington, D.C. 20231 on July 2, 2001.

**Dated:** July 2, 2001

  
Janet Grossman



日 本 国 特 許 庁  
JAPAN PATENT OFFICE

JC979 U.S. PTO

09/897323



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年 7月 5日

出 願 番 号

Application Number:

特願2000-204112

出 願 人

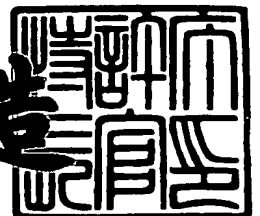
Applicant(s):

日本電気株式会社

2001年 5月25日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3043398

【書類名】 特許願

【整理番号】 60301686

【提出日】 平成12年 7月 5日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 12/54  
H04L 12/58  
G06F 13/00

【発明者】

【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

【氏名】 東 富彦

【特許出願人】

【識別番号】 000004237

【氏名又は名称】 日本電気株式会社

【代理人】

【識別番号】 100080816

【弁理士】

【氏名又は名称】 加藤 朝道

【電話番号】 045-476-1131

【手数料の表示】

【予納台帳番号】 030362

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9304371

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 セキュアメールプロキシシステム及び方法並びに記録媒体

【特許請求の範囲】

【請求項 1】

L A N（ローカルエリアネットワーク）上のメールサーバとインターネットとの間に、前記インターネットへ送信する電子メールの暗号化と署名の添付、及び前記インターネットからの署名付き暗号メールの改竄の有無の検査と復号化など、セキュリティ管理に必要な処理を代行するプロキシ装置を備えたことを特徴とするセキュアメールプロキシシステム。

【請求項 2】

L A N（ローカルエリアネットワーク）上のメールサーバとインターネットとの間に、電子メールのセキュリティに関する処理を行うセキュアメールプロキシ装置を配置し、

前記セキュアメールプロキシ装置が、前記メールサーバから受け取った電子メールを暗号化し署名を添付して前記インターネットへ送出する手段と、

前記インターネットから証明付き暗号化メールが前記メールサーバ宛てに送信された場合に、該メールの改竄の有無を検出し、改竄されていない場合に、暗号化メールを復号して前記メールサーバに送信する手段と、

を備え、

ユーザが利用するメールサーバ、メールクライアント、ユーザ端末などの種類やセキュリティ機能の実装の有無に依存することなく、インターネットにおける電子メールのセキュリティを確保可能としたことを特徴とするセキュアメールプロキシシステム。

【請求項 3】

L A N（ローカルエリアネットワーク）上のメールサーバとインターネットとの間に、電子メールのセキュリティに関する処理を行うセキュアメールプロキシ装置を配置し、

メールクライアントから前記メールサーバに対して平文の電子メールを送信し

前記メールサーバは、前記電子メールの宛先が前記 LAN 内であるか否かを検査し、前記 LAN 外宛ての電子メールは、平文のまま前記セキュアメールプロキシ装置へ送信し、

前記セキュアメールプロキシ装置が、前記メールサーバから受信した平文の電子メールに対して、メール受信者だけが前記電子メールを復号化できるように暗号化する手段と、

暗号化メールにメール発信者の署名を付けて前記インターネットへ署名済みの暗号化された電子メールを送出する手段と、

署名付きの暗号化された電子メールが前記インターネットを通して前記メールサーバ宛てに送信されてきた場合に、前記電子メールが改竄されていないかどうかをチェックし、前記電子メールが改竄されていない場合には、前記暗号化メールを復号化し平文メールにした上で、前記メールサーバへ配送する手段と、

前記電子メールが改竄されている場合には、前記電子メールの受信を拒否することで改竄された電子メールが前記 LAN 内に入ることを防止する手段と、  
を備え、

前記メールクライアントは、前記メールサーバに受信した電子メールを要求し、前記メールサーバから平文の電子メールを受け取る、ことを特徴とするセキュアメールプロキシシステム。

#### 【請求項 4】

LAN（ローカルエリアネットワーク）と、前記 LAN に接続するメールサーバと、前記メールサーバとインターネットとの間に設けられ、電子メールのセキュリティに関する処理を行うセキュアメールプロキシ装置と、を有するセキュアメールプロキシシステムであって、

前記セキュアメールプロキシ装置が、

電子メールアドレスと該電子メールアドレスに対応する秘密鍵との組を記憶した秘密鍵記憶手段と、

電子メールアドレスと該電子メールアドレスに対応する公開鍵との組を記憶している公開鍵記憶手段とを備え、

前記秘密鍵は、電子メールに対して発信者の署名を付ける場合と、前記 LAN

内の電子メールアドレスに対して送信されてきた暗号化メールを復号化する場合に使用され、

前記公開鍵は、電子メールの宛先に指定された電子メールアドレスのユーザにしか読めないようにメールを暗号化する場合と、メールが改竄されていないかどうかをチェックする場合に使用され、

電子メールの宛先の電子メールアドレスに対応する公開鍵を前記公開鍵記憶部から取得し、前記メールサーバからの平文メールを公開鍵で暗号化するメール暗号化手段と、

電子メール発信者のメールアドレスに対応する秘密鍵を前記秘密鍵記憶部から取得し、前記電子メールのメッセージダイジェストを計算し、その値を、秘密鍵で暗号化した上で電子メールに発信者の署名として添付するメール署名添付手段と、

電子メールの宛先の電子メールアドレスに対応する秘密鍵を前記秘密鍵記憶部から取得し、暗号化されているメールを秘密鍵で復号化するメール復号化手段と、

電子メール発信者のメールアドレスに対応する公開鍵を前記公開鍵記憶部から取得し、メールに添付されている署名を、公開鍵で復号化し、署名の値とメールのメッセージダイジェストとを比較することによって、メールが改竄されていないかどうかを検査するメール署名検査手段と、

前記メールサーバから平文の電子メールを受信し、前記メール暗号化手段と前記メール署名添付手段で作成された署名付き暗号化メールを前記インターネットに送信するとともに、前記インターネットから署名付き暗号化メールを受信し、前記メール署名検査手段と前記メール復号化手段を介して得られた平文メールを前記メールサーバへ送信するデータ通信手段と、

を備えたことを特徴とするセキュアメールプロキシシステム。

#### 【請求項 5】

LAN（ローカルエリアネットワーク）に接続するメールサーバとインターネットとの間に配置され、電子メールのセキュリティに関する処理を行うセキュアメールプロキシ装置が

電子メールアドレスと該電子メールアドレスに対応する秘密鍵との組を記憶した秘密鍵記憶部と、

電子メールアドレスと該電子メールアドレスに対応する公開鍵との組を記憶している公開鍵記憶部を含む記憶装置を備え、

前記秘密鍵は、電子メールに対して発信者の署名を付ける場合と、前記 LAN 内の電子メールアドレスに対して送信されてきた暗号化メールを復号化する場合に使用され、

前記公開鍵は、電子メールの宛先に指定された電子メールアドレスのユーザにしか読めないようにメールを暗号化する場合と、メールが改竄されていないかどうかをチェックする場合に使用され、

電子メールの宛先の電子メールアドレスに対応する公開鍵を前記公開鍵記憶部から取得し、前記メールサーバからの平文メールを公開鍵で暗号化するメール暗号化手段と、

電子メール発信者のメールアドレスに対応する秘密鍵を前記秘密鍵記憶部から取得し、前記電子メールのメッセージダイジェストを計算し、その値を、秘密鍵で暗号化した上で電子メールに発信者の署名として添付するメール署名添付手段と、

電子メールの宛先の電子メールアドレスに対応する秘密鍵を前記秘密鍵記憶部から取得し、暗号化されているメールを秘密鍵で復号化するメール復号化手段と、

電子メール発信者のメールアドレスに対応する公開鍵を前記公開鍵記憶部から取得し、電子メールに添付されている署名を、公開鍵で復号化し、署名の値と電子メールのメッセージダイジェストとを比較することによって、メールが改竄されていないかどうかを検査するメール署名検査手段と、

前記メールサーバから平文の電子メールを受信し、前記メール暗号化手段と前記メール署名添付手段で作成された、署名付き暗号化メールを前記インターネットに送信するとともに、前記インターネットから署名付き暗号化メールを受信し、前記メール署名検査手段と前記メール復号化手段を介して得られた平文メールを前記メールサーバへ送信するデータ通信手段と、

を含むデータ処理装置を備えたことを特徴とするセキュアメールプロキシ装置

【請求項 6】

前記メールクライアントが、前記 LAN に直接接続されるか、あるいは、公衆回線網、無線通信網、もしくはケーブルテレビジョン（CATV）網の少なくともいずれかを介して、前記 LAN の前記メールサーバに接続される、ことを特徴とする請求項 3 又は 4 記載のセキュアメールプロキシシステム。

【請求項 7】

前記セキュアメールプロキシ装置には、電子メールアドレスと該電子メールアドレスに対応する秘密鍵との組を記憶した秘密鍵記憶手段と、電子メールアドレスと該電子メールアドレスに対応する公開鍵との組を記憶している公開鍵記憶手段を設けず、

電子メールアドレスと該電子メールアドレスに対応する秘密鍵の組を管理するための専用の鍵管理サーバを備えるとともに、電子メールアドレスと該電子メールアドレスに対応する公開鍵の組を管理するためのディレクトリサーバを備え、

前記セキュアメールプロキシ装置の前記メール暗号化手段、前記メール署名添付手段、前記メール復号化手段、および、前記メール署名検査手段は、それぞれ、公開鍵、秘密鍵を、前記ディレクトリサーバ、および、前記鍵管理サーバをアクセスして取得する、ことを特徴とする請求項 4 記載のセキュアメールプロキシシステム。

【請求項 8】

LAN（ローカルエリアネットワーク）上のメールサーバとインターネットとの間に、電子メールのセキュリティに関する処理を行うセキュアメールプロキシを設け、

前記インターネットへ送信する電子メールの暗号化と署名の添付、及び、前記インターネットから前記メールサーバ宛の電子メールの改竄の有無の検査と復号化を含む、電子メールのセキュリティ管理に必要な処理を、前記インターネットの接続点に配置された前記セキュアメールプロキシが代行して行うことで、ユーザが利用するメールサーバ、メールクライアント、ユーザ端末などの種類やセキ



セキュリティ機能の実装の有無に依存することなく、インターネットにおける電子メールのセキュリティを確保可能としたことを特徴とする電子メールのセキュリティ管理方法。

【請求項 9】

L A N（ローカルエリアネットワーク）に接続するメールサーバとインターネットとの間にセキュアメールプロキシを配置し、

メールクライアントからの平文の電子メールを受け取った前記メールサーバは、前記電子メールの宛先が前記 L A N 内であるか否かを検査し、前記 L A N 外宛の電子メールは平文のまま前記セキュアメールプロキシへ送り、

前記セキュアメールプロキシは前記メールサーバからの平文の電子メールに対して、メール受信者だけが前記電子メールを復号化できるように暗号化し、

さらに、メール発信者の署名を付けてインターネットへ署名済みの暗号化された電子メールを送出し、

署名済みの暗号化された電子メールが前記インターネットを通して前記メールサーバ宛てに送信されてきた場合に、前記電子メールの改竄の有無をチェックし、

前記電子メールが改竄されていない場合には、暗号化されている前記電子メールを復号化して平文メールにした上で前記メールサーバへ配送し、

一方、前記電子メールが改竄されている場合には前記電子メールの受信を拒否し、改竄された電子メールが前記 L A N 内に入ることを防止し、

ユーザは前記メールクライアントを利用して、前記メールサーバに受信した電子メールを要求し、前記メールサーバから平文の電子メールを受け取る、ことを特徴とする電子メールのセキュリティ管理方法。

【請求項 1 0】

ユーザが、メールクライアントを利用して電子メールを作成し、平文のままメールサーバに送信するステップと、

前記メールサーバは、前記メールクライアントから送信された電子メールの宛先が、前記メールサーバが接続される L A N（ローカルエリアネットワーク）内であるか否かをチェックするステップと、

前記電子メールの宛先が前記LAN外である場合には平文の電子メールをセキュアメールプロキシへ配送するステップと、

前記セキュアメールプロキシは、前記メールサーバから平文の電子メールを受信し、前記電子メールの宛先の電子メールアドレスに対応する公開鍵を、電子メールアドレスと該電子メールアドレスに対応する公開鍵との組を記憶している公開鍵記憶部から取得し、前記平文の電子メールを公開鍵で暗号化するステップと、

前記セキュアメールプロキシは、前記電子メールの発信者の電子メールアドレスに対応する秘密鍵を、電子メールアドレスと該電子メールアドレスに対応する秘密鍵との組を記憶した秘密鍵記憶部から取得し、前記電子メールのメッセージダイジェストを計算し、その値を秘密鍵で暗号化した上で、前記電子メールに、発信者の署名として添付するステップと、

前記セキュアメールプロキシが、署名付き暗号化メールをインターネットへ送り出すステップと、

を含む、ことを特徴とする電子メールのセキュリティ管理方法。

#### 【請求項 1 1】

前記セキュアメールプロキシが、前記インターネットから署名付きの暗号化された電子メールを受信するステップと、

前記セキュアメールプロキシが、電子メール発信者のメールアドレスに対応する公開鍵を前記公開鍵記憶部から取得し、前記電子メールに添付されている署名を公開鍵で復号化するステップと、

署名の値と前記電子メールのメッセージダイジェストとを比較することによって、前記電子メールが改竄されていないかどうかを検査するステップと、

前記電子メールが改竄されていない場合には、前記セキュアメールプロキシは、前記電子メールの宛先のメールアドレスに対応する秘密鍵を前記秘密鍵記憶部から取得し、暗号化されている前記電子メールを秘密鍵で復号化するステップと、

平文に復号された電子メールを前記LAN内の前記メールサーバへ配送するステップと、

前記電子メールが改竄されている場合には、前記セキュアメールプロキシはメールの受信を拒否し、改竄された電子メールが前記LAN内に入るのを防止するステップと、

前記メールサーバが前記セキュアメールプロキシから平文の電子メールを受信するステップと、

ユーザは前記メールクライアントを利用して前記メールサーバに対して受信したメールを要求し、前記メールサーバから平文メールを受け取るステップと、

を含む、ことを特徴とする請求項10記載の電子メールのセキュリティ管理方法。

【請求項12】

LAN（ローカルエリアネットワーク）に接続するメールサーバとインターネットとの間に電子メールのセキュリティに関する処理を行うプロキシ装置において、

電子メールアドレスと、それに対応する秘密鍵との組を記憶した秘密鍵記憶部と、

電子メールアドレスと、それに対応する公開鍵との組を記憶している公開鍵記憶部を備えた記憶装置を備え、

前記秘密鍵は、電子メールに対して発信者の署名を付ける場合と、前記LAN内の電子メールアドレスに対して送信されてきた暗号化メールを復号化する場合に使用され、

前記公開鍵は、電子メールの宛先に指定された電子メールアドレスのユーザにしか読めないように電子メールを暗号化する場合と、電子メールが改竄されていないかどうかをチェックする場合に使用され、

（a）電子メールの宛先の電子メールアドレスに対応する公開鍵を前記公開鍵記憶部から取得し、平文メールを公開鍵で暗号化するメール暗号化処理と、

（b）電子メール発信者のメールアドレスに対応する秘密鍵を前記秘密鍵記憶部から取得し、前記電子メールのメッセージダイジェストを計算し、その値を、秘密鍵で暗号化した上で電子メールに発信者の署名として添付するメール署名添付処理と、

(c) 電子メールの宛先の電子メールアドレスに対応する秘密鍵を前記秘密鍵記憶部から取得し、暗号化されているメールを秘密鍵で復号化するメール復号化処理と、

(d) 電子メール発信者のメールアドレスに対応する公開鍵を前記公開鍵記憶部から取得し、メールに添付されている署名を、公開鍵で復号化し、署名の値とメールのメッセージダイジェストとを比較することによって、メールが改竄されていないかどうかを検査するメール署名検査処理と、

(e) 前記メールサーバから平文メールを受信し、署名付き暗号化メールをインターネットに送信するとともに、前記インターネットから署名付き暗号化メールを受信し、前記メールサーバへ平文メールを送信するデータ通信処理と、

の前記(a)乃至(e)の処理をプロキシ装置を構成するコンピュータに実行させるためのプログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、電子メールのメールのセキュリティを確保するシステム及び方法並びにプログラムを記録した記録媒体に関する。

【0002】

【従来の技術】

電子メールのセキュリティを確保するためのシステムとしては、暗号化したメッセージをMIME形式で転送するS/MIME (Secure/Multipurpose Internet Mail Extension; エスマイム; RSAデータセキュリティ社開発)、PGP (Pretty Good Privacy: ピージーピー; PGP社が開発した暗号化プログラム、メールの内容を送信相手の公開鍵で暗号化して送信する) 等のセキュリティ機能を具備したメールクライアントが広く一般的に利用されている。

【0003】

セキュリティを有効に機能させるためには、自分の秘密鍵や送信相手のデジタル証明書等を、自分が使用する端末に事前にインストールする方法が、一般的に採用されている。

【 0 0 0 4 】

【発明が解決しようとする課題】

しかしながら、従来のシステムは、次のような問題点を有している。

【 0 0 0 5 】

メールを送受信する端末が、従来の P C ( パーソナルコンピュータ ) から、携帯電話機や、携帯情報端末、 F A X ( ファクシミリ ) などの端末へ広がるとともに、セキュリティ機能を備えたメールクライアントを持たない端末が増加し、インターネット上でのメールのセキュリティを確保することができなくなっていることである。

【 0 0 0 6 】

そして、急速に普及している携帯電話においては、端末側でのセキュリティ機能の実装が困難であり、このため、ビジネスでの利用を妨げる大きな原因ともなっている。

【 0 0 0 7 】

したがって本発明は、上記問題点に鑑みてなされたものであって、その目的は、クライアント側のセキュリティ機能の実装の有無に依存することなく、インターネットにおける電子メールのセキュリティを確保可能とするシステム及び方法並びに記録媒体を提供することにある。

【 0 0 0 8 】

【課題を解決するための手段】

前記目的を達成する本発明は、メールサーバとインターネットとの間に電子メールのセキュリティに関する処理を行うプロキシ装置を配置し、前記プロキシ装置が、電子メールの暗号化、復号化、及び、署名の添付、改竄の検出を行う手段を備え、ユーザが利用するメールサーバ、メールクライアント、ユーザ端末などの種類やセキュリティ機能の実装の有無に依存することなく、インターネットにおける電子メールのセキュリティ確保するようにしたものである。

【 0 0 0 9 】

本発明は、メールサーバとインターネットとの間に電子メールのセキュリティに関する処理を行うセキュアメールプロキシ装置を配置し、 L A N に接続されて

いるメールクライアントからメールサーバに対して、署名も暗号化もされていない平文メールを送信し、前記メールサーバは、メールの宛先がLAN内であるか否かを検査し、LAN外宛てのメールだけを平文のまま前記セキュアメールプロキシ装置へ送り、前記セキュアメールプロキシ装置は、前記メールサーバから受信した平文メールに対して、メール受信者だけがメールを復号化できるように暗号化する手段と、メール発信者の署名を付けて、インターネットへ、署名済み暗号化メールを送出する手段と、署名済み暗号化メールがインターネットを通してメールサーバ宛てに送信されてきた場合に、メールが改竄されていないかどうかをチェックし、メールが改竄されていない場合には、前記セキュアメールプロキシが暗号化メールを復号化して、平文メールにした上で、前記メールサーバへ配送する手段と、メールが改竄されている場合には、メールの受信を拒否し、改竄されたメールがLAN内に入ることを防止する手段と、を備え、ユーザはメールクライアントを利用して、前記メールサーバに受信したメールを要求し、前記メールサーバから平文メールを受け取る。

【0010】

#### 【発明の実施の形態】

本発明の実施の形態について説明する。LAN（ローカルエリアネットワーク）上のメールサーバとインターネットとの間に電子メールのセキュリティに関する処理を行うプロキシ（セキュアメールプロキシ）を配置し、このプロキシにおいて、電子メールの暗号化／復号化や、署名の添付／改竄の検出等を実行することにより、ユーザが利用するメールサーバ、メールクライアント、ユーザ端末などの種類やセキュリティ機能の実装の有無に依存することなく、インターネットにおける電子メールのセキュリティ確保を実現したものである。

【0011】

図1において、ユーザは、LAN1に接続されているメールクライアント3を利用して、メールサーバ2に対して、署名も暗号化もされていない平文メールを送信する。

【0012】

メールサーバ2は、電子メール（単に「メール」ともいう）の宛先がLAN1

内であるか否かを検査し、LAN 1 外宛てのメールだけを、平文のまま、セキュアメールプロキシ (secure mail proxy) 4 へ送る。

【 0 0 1 3 】

セキュアメールプロキシ 4 は、メールサーバ 2 から受信した平文メールに対して、メール受信者だけがメールを復号化できるように、暗号化し、メール発信者の署名を付けて、インターネット 5 へ、署名済み暗号化メールを送り出す。

【 0 0 1 4 】

署名済み暗号化メールがインターネット 5 を通してメールサーバ 2 宛てに送信されてきた場合には、セキュアメールプロキシ 4 は、メールが改竄されていないかどうかをチェックする。

【 0 0 1 5 】

メールが改竄されていない場合には、セキュアメールプロキシ 4 が暗号化メールを復号化して、平文メールにした上で、メールサーバ 2 へ配送する。

【 0 0 1 6 】

メールが改竄されている場合には、セキュアメールプロキシ 4 は、メールの受信を拒否し、改竄されたメールが、LAN 1 内に入るのを防止する。

【 0 0 1 7 】

ユーザは、メールクライアント 3 を利用して、メールサーバ 2 に受信したメールを要求し、メールサーバ 2 から平文メールを受け取る。

【 0 0 1 8 】

【実施例】

上記した本発明の実施の形態についてさらに詳細に説明すべく、本発明の実施例について図面を参照して以下に説明する。図 1 は、本発明の一実施例のシステム構成を示す図である。図 1 を参照すると、本発明の一実施例は、イーサネットなどのローカルエリアネットワークである LAN 1 と、LAN 1 に接続されている情報処理装置であるメールサーバ 2 と、パーソナルコンピュータ、携帯電話、携帯情報端末、FAX などの装置の上で動作するメールクライアント 3 と、メールサーバ 2 とインターネット 5 との接続を仲介する情報処理装置であるセキュアメールプロキシ 4 と、インターネット 5 とを含む。

【 0 0 1 9 】

図 2 は、本発明の一実施例におけるセキュアメールプロキシ 4 の構成の一例を示す図である。図 2 を参照すると、セキュアメールプロキシ 4 は、プログラム制御により動作するデータ処理装置 4 1 と、情報を記憶する記憶装置 4 2 と、を含む。

【 0 0 2 0 】

記憶装置 4 2 は、秘密鍵記憶部 4 2 1 と公開鍵記憶部 4 2 2 とを備えている。

【 0 0 2 1 】

秘密鍵記憶部 4 2 1 には、電子メールアドレス（単に「メールアドレス」ともいう）と、それに対応する秘密鍵との組が記憶されている。秘密鍵は、電子メールに対して、発信者の署名を付ける場合と、LAN 1 内のメールアドレスに対して送信されてきた暗号化メールを復号化する場合に使用される。

【 0 0 2 2 】

公開鍵記憶部 4 2 2 には、電子メールアドレスと、それに対応する公開鍵との組が記憶されている。

【 0 0 2 3 】

公開鍵は、電子メールの宛先に指定された電子メールアドレスのユーザにしか読めないように電子メールを暗号化する場合と、電子メールが改竄されていないかどうかをチェックする場合に使用される。

【 0 0 2 4 】

データ処理装置 4 1 は、メール暗号化手段 4 1 1 と、メール復号化手段 4 1 2 と、メール署名添付手段 4 1 3 と、メール署名検査手段 4 1 4 と、データ通信手段 4 1 5 と、を備えている。

【 0 0 2 5 】

メール暗号化手段 4 1 1 は、電子メールの宛先の電子メールアドレスに対応する公開鍵を公開鍵記憶部 4 2 2 から取得し、平文メールを公開鍵で暗号化する。

【 0 0 2 6 】

メール復号化手段 4 1 2 は、電子メールの宛先の電子メールアドレスに対応する秘密鍵を秘密鍵記憶部 4 2 1 から取得し、暗号化されている電子メールを秘密



鍵で復号化する。

【 0 0 2 7 】

メール署名添付手段 4 1 3 は、電子メール発信者の電子メールアドレスに対応する秘密鍵を秘密鍵記憶部 4 2 1 から取得し、電子メールのメッセージダイジェスト（ハッシュ値）を計算し、その値を、秘密鍵で暗号化した上で、電子メールに発信者の署名として添付する。

【 0 0 2 8 】

メール署名検査手段 4 1 4 は、電子メール発信者の電子メールアドレスに対応する公開鍵を公開鍵記憶部 4 2 2 から取得し、電子メールに添付されている署名を、公開鍵で復号化し、署名の値と電子メールのメッセージダイジェスト（ハッシュ値）とを比較することによって、電子メールが改竄されていないかどうかを検査する。

【 0 0 2 9 】

データ通信手段 4 1 5 は、メールサーバ 2 から平文メールを受信し、署名付き暗号化メールをインターネット 5 に送信するとともに、インターネット 5 から署名付き暗号化メールを受信し、メールサーバ 2 へ平文メールを送信する。

【 0 0 3 0 】

本発明の一実施例において、メール暗号化手段 4 1 1、メール復号化手段 4 1 2、メール署名添付手段 4 1 3、メール署名検査手段 4 1 4、データ通信手段 4 1 5 はデータ処理装置 4 1 で実行されるプログラムによりその処理・機能が実現される。この場合、該プログラムを記録した記録媒体（磁気ディスク、磁気テープ、光ディスク、あるいは半導体メモリ等）から該プログラムをデータ処理装置 4 1 に読み出して実行することで、本発明に係るセキュアメールプロキシ装置を実施することができる。

【 0 0 3 1 】

次に図 1 乃至図 6 を参照して、本発明の一実施例の動作について詳細に説明する。

【 0 0 3 2 】

図 3 は、本発明の一実施例において、メールクライアント 3 からの電子メール

送信時の動作について説明する流れ図である。まず、メールクライアント 3 からの電子メールの送信について説明する。

【 0 0 3 3 】

ユーザは、メールクライアント 3 を利用して電子メールを作成し、平文のままメールサーバ 2 に送信する（ステップ A 1）。

【 0 0 3 4 】

メールサーバ 2 は、メールクライアント 3 から送信されたメールの宛先が LAN 1 内であるか否かをチェックし（ステップ A 2）、LAN 1 外である場合には平文メールをセキュアメールプロキシ 4 へ配送し（ステップ A 3）、LAN 1 内である場合には、LAN 1 に接続されているメールサーバ 2 に、平文のまま電子メールを配送する（ステップ A 4）。

【 0 0 3 5 】

セキュアメールプロキシ 4 は、データ通信手段 4 1 5 により、メールサーバ 2 から平文メールを受信し、メール暗号化手段 4 1 1 により、電子メールの宛先のメールアドレスに対応する公開鍵を公開鍵記憶部 4 2 2 から取得し、平文メールを公開鍵で、暗号化する（ステップ A 5）。

【 0 0 3 6 】

図 6 は、公開鍵記憶部 4 2 2 に記憶されている電子メールアドレスと公開鍵の組情報例を示す図である。

【 0 0 3 7 】

メールの宛先のメールアドレスが、“u-suzuki@abc.com” である場合には、対応する公開鍵として、“111…001” が暗号化に利用される。

【 0 0 3 8 】

次に、セキュアメールプロキシ 4 は、メール署名添付手段 4 1 3 により、メール発信者の電子メールアドレスに対応する秘密鍵を秘密鍵記憶部 4 2 1 から取得し、当該電子メールのメッセージダイジェスト（ハッシュ値）を計算し、その値を秘密鍵で暗号化した上で、メール発信者の署名として添付する（ステップ A 6）。

【 0 0 3 9 】

図 5 は、秘密鍵記憶部 4 2 1 に記憶されている電子メールアドレスと秘密鍵の組情報の例を示す図である。メール発信者の電子メールアドレスが” t-azuma@nec.co.jp” である場合には、対応する秘密鍵として” 101…001” が署名に利用される。

## 【 0 0 4 0 】

最後に、セキュアメールプロキシ 4 は、データ通信手段 4 1 5 により署名付き暗号化メールをインターネット 5 へ送り出す（ステップ A 7）。

## 【 0 0 4 1 】

図 4 は、本発明の一実施例において、インターネット 5 から署名付き暗号化メールを受信した場合に動作を説明する図である。インターネット 5 から署名付き暗号化メールを受信時の動作について以下に説明する。

## 【 0 0 4 2 】

セキュアメールプロキシ 4 は、データ通信手段 4 1 5 により、インターネット 5 から署名付き暗号化メールを受信する（ステップ B 1）。

## 【 0 0 4 3 】

セキュアメールプロキシ 4 は、メール署名検査手段 4 1 4 により、メール発信者のメールアドレスに対応する公開鍵を公開鍵記憶部 4 2 2 から取得し、電子メールに添付されている署名を公開鍵で復号化し（ステップ B 2）、署名の値と、電子メールのメッセージダイジェスト（ハッシュ値）とを比較することによって、電子メールが改竄されていないかどうかを検査する（ステップ B 3）。

## 【 0 0 4 4 】

図 6 の例では、メール発信者のメールアドレスが、” u-suzuki@abc.com” である場合には、対応する公開鍵として、” 111…001” が署名の復号化に利用される。

## 【 0 0 4 5 】

電子メールが改竄されていない場合には、セキュアメールプロキシ 4 は、メール復号化手段 4 1 2 により、電子メールの宛先のメールアドレスに対応する秘密鍵を秘密鍵記憶部 4 2 1 から取得し、暗号化されている電子メールを秘密鍵で復号化する。

【 0 0 4 6 】

図 5 に示す例では、メール受信者のメールアドレスが” t-azuma@nec.co.jp” である場合には、対応する秘密鍵として” 101…001” が暗号化メッセージの復号化に利用される。

【 0 0 4 7 】

平文に復号されたメッセージは、データ通信手段 4 1 5 により、LAN 1 内のメールサーバ 2 へ配送される（ステップ B 5）。

【 0 0 4 8 】

電子メールが改竄されている場合には、セキュアメールプロキシ 4 はメールの受信を拒否し、改竄されたメールが LAN 1 内に入ることを防止する（ステップ B 6）。

【 0 0 4 9 】

メールサーバ 2 は、セキュアメールプロキシ 4 から平文メールを受信し（ステップ B 7）、メールクライアント 3 からメールの要求があった場合に、平文メールをメールクライアント返却する（ステップ B 9）。

【 0 0 5 0 】

ユーザは、メールクライアント 3 を利用してメールサーバ 2 に対して受信したメールを要求し（ステップ B 8）、メールサーバ 2 から平文メールを受け取る（ステップ B 1 0）。

【 0 0 5 1 】

次に、本発明の他の実施例について説明する。

【 0 0 5 2 】

図 7 は、本発明の第 2 の実施例の構成を示す図である。図 7 参照すると、本発明の第 2 の実施例において、LAN 1 に接続する手段として、前記実施例のように、直接 LAN 1 に接続するほかに、例えば、公衆回線網 6 1、無線通信網 6 2、および CATV 網 6 3 のうち少なくともいずれか一つ又は全てを用いてもよい。

【 0 0 5 3 】

公衆回線網 6 1 を介して LAN 1 に接続する例としては、インターネット接続

プロバイタ（ISP）等を利用して、ダイヤルアップ接続する形態がある。

【0054】

無線通信網62を介してLAN1に接続する例としては、携帯電話機からインターネット接続サービスを提供している携帯電話業者を介して、接続する形態がある。

【0055】

CATV（有線テレビジョン）網63を介してLAN1に接続する例としては、インターネット接続サービスを提供しているCATV会社を介して接続する形態がある。

【0056】

さらに、本発明の第3の実施例について説明する。図8は、本発明の第3の実施例の構成を示す図である。図8を参照すると、本実施例は、鍵管理サーバ7およびディレクトリサーバ8を有しており、セキュアメールプロキシ4において秘密鍵記憶部421および公開鍵記憶部422を備えていない。

【0057】

鍵管理サーバ7は、図5に示すような電子メールアドレスと秘密鍵の組を管理するための専用のサーバであり、ディレクトリサーバ8は、図6に示すような電子メールアドレスと公開鍵の組を管理するための専用のサーバである。

【0058】

本実施例では、セキュアメールプロキシ4のメール暗号化手段411およびメール署名検査手段414は、ディレクトリサーバ8から、公開鍵を入手する。

【0059】

また、メール復号化手段412およびメール署名添付手段413は、鍵管理サーバ7から秘密鍵を入手する。なお、本発明の第3の実施例においては、セキュアメールプロキシ4が、公開鍵、秘密鍵を、それぞれ、ディレクトリサーバ8、鍵管理サーバ7から取得すること以外、その処理手順は、図3及び図4に示した手順と同様とされている。

【0060】

【発明の効果】

以上説明したように、本発明によれば下記記載の効果を奏する。

【 0 0 6 1 】

本発明の第 1 の効果は、メールを送受信する端末に特別なソフトや装置を組みこむことなく、インターネット上でのメールのセキュリティを確保することができるということである。

【 0 0 6 2 】

特に、急速に普及している携帯電話や携帯情報端末をメールクライアントの端末とするシステムにおいては、対象とする機種が多種多様であることと、既に出荷されている台数が膨大であることから、本発明によるセキュリティ確保の効果は顕著である。

【 0 0 6 3 】

その理由は、本発明においては、メールのセキュリティを確保するために必要な処理をユーザ端末側に持たせるのではなく、インターネットとの接続点に配置したプロキシにすべて代行させているためである。そして、社内 LAN などのインターネットと接続しているポイントの内側では、インターネット上に比べて、セキュリティに対する脅威ははるかに少ないため、インターネットと接続しているポイントにセキュリティの機能を集約させることができるためである。

【 0 0 6 4 】

本発明の第 2 の効果は、セキュリティ確保に必要な管理コストを大幅に低減できる、ということである。特に、複数の端末を使うユーザにとっては、端末ごとにセキュリティの設定をする必要がなくなるため効果は顕著である。

【 0 0 6 5 】

その理由は、本発明においては、セキュリティ確保に必要な秘密鍵や公開鍵などをプロキシで一元管理することにより、クライアント毎のセキュリティ設定を不要にしたためである。

【図面の簡単な説明】

【図 1】

本発明の一実施例のシステム構成を示す図である。

【図 2】

本発明の一実施例におけるセキュアメールプロキシの構成の一例を示す図である。

【図 3】

本発明の一実施例におけるメールクライアントからのメール送信時の動作について説明する流れ図である。

【図 4】

本発明の一実施例におけるインターネットから署名付き暗号化メールを受信した場合に動作を説明する図である。

【図 5】

本発明の一実施例における秘密鍵記憶部に記憶されている電子メールアドレスと秘密鍵の組情報の例を示す図である。

【図 6】

本発明の一実施例における公開鍵記憶部に記憶されている電子メールアドレスと公開鍵の組情報例を示す図である。

【図 7】

本発明の第 2 の実施例のシステム構成を示す図である。

【図 8】

本発明の第 3 の実施例のシステム構成を示す図である。

【符号の説明】

- 1    L A N
- 2    メールサーバ
- 3    メールクライアント
- 4    セキュアメールプロキシ
  - 4 1   データ処理装置
    - 4 1 1   メール暗号化手段
    - 4 1 2   メール復号化手段
    - 4 1 3   メール署名添付手段
    - 4 1 4   メール署名検査手段
    - 4 1 5   データ通信手段

4 2 記憶装置

4 2 1 秘密鍵記憶部

4 2 2 公開鍵記憶部

5 インターネット

6 1 ~ 6 2 公衆回線網

6 3 C A T V 網

7 鍵管理サーバ

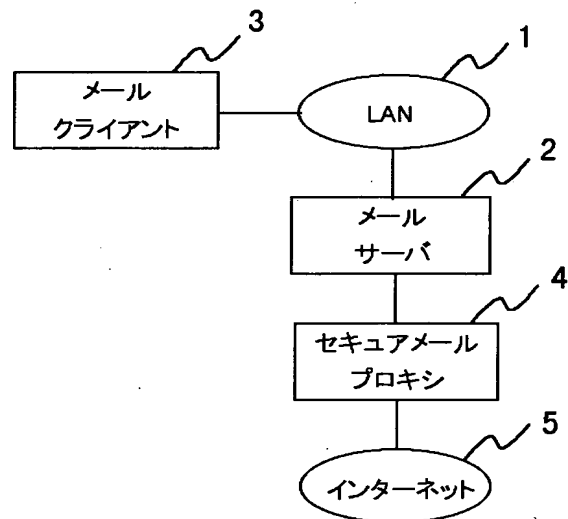
8 ディレクトリサーバ



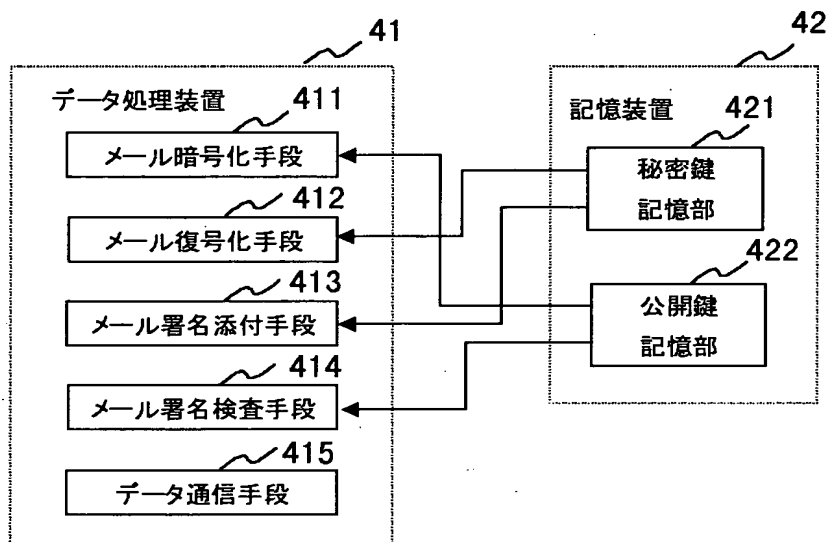
【書類名】

図面

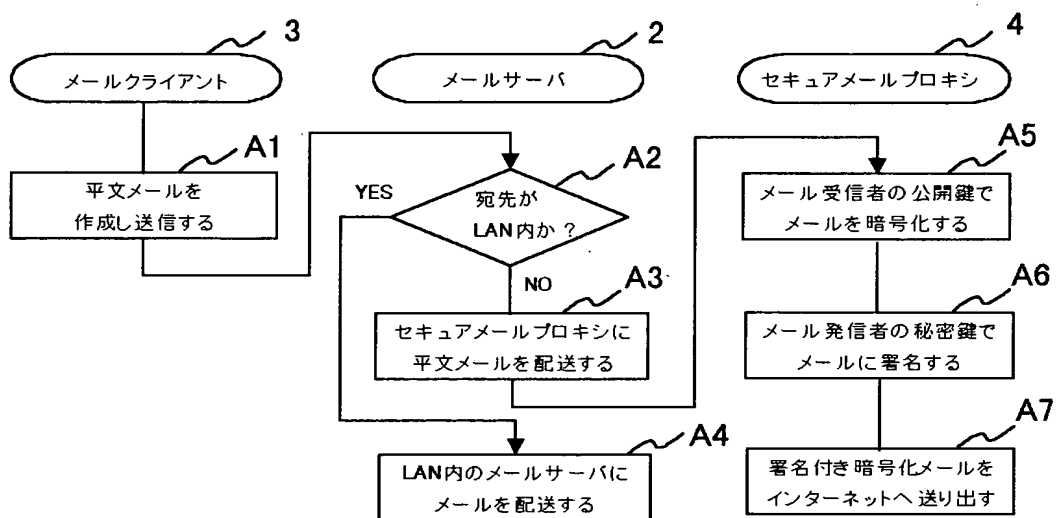
【図 1】



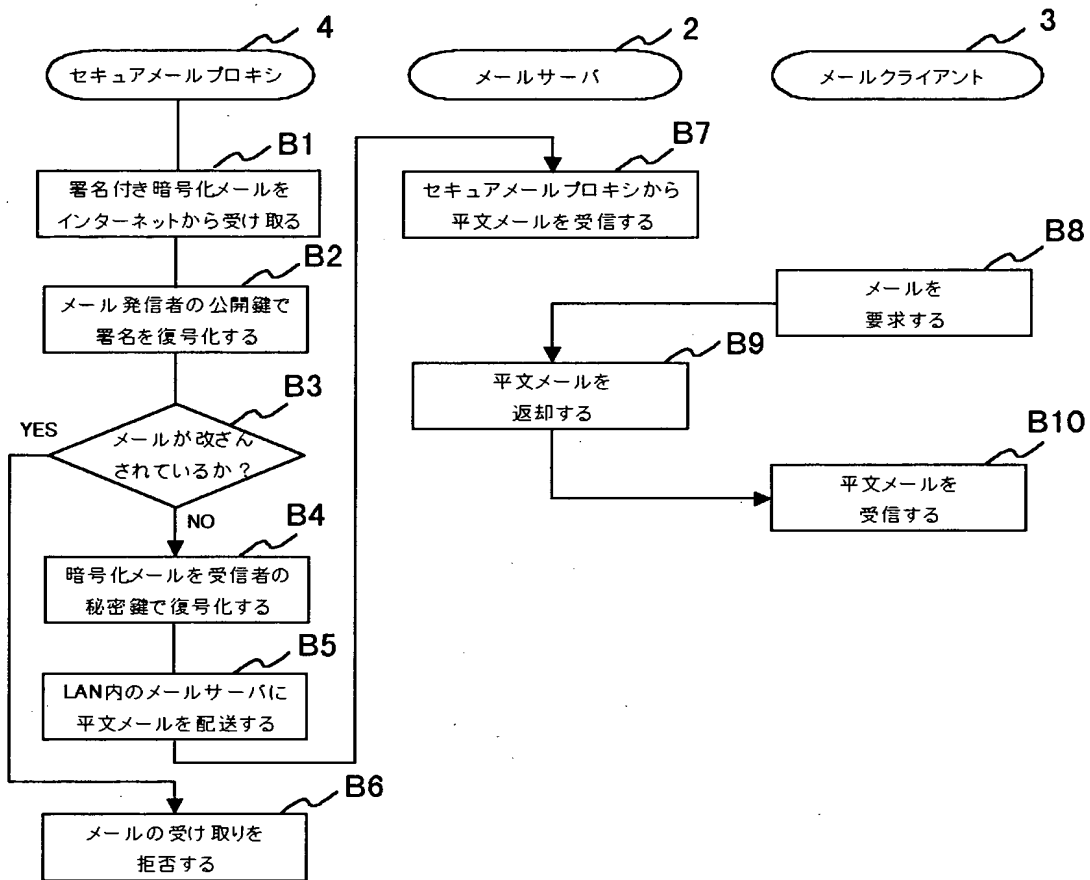
【図 2】



【図 3】



【図4】



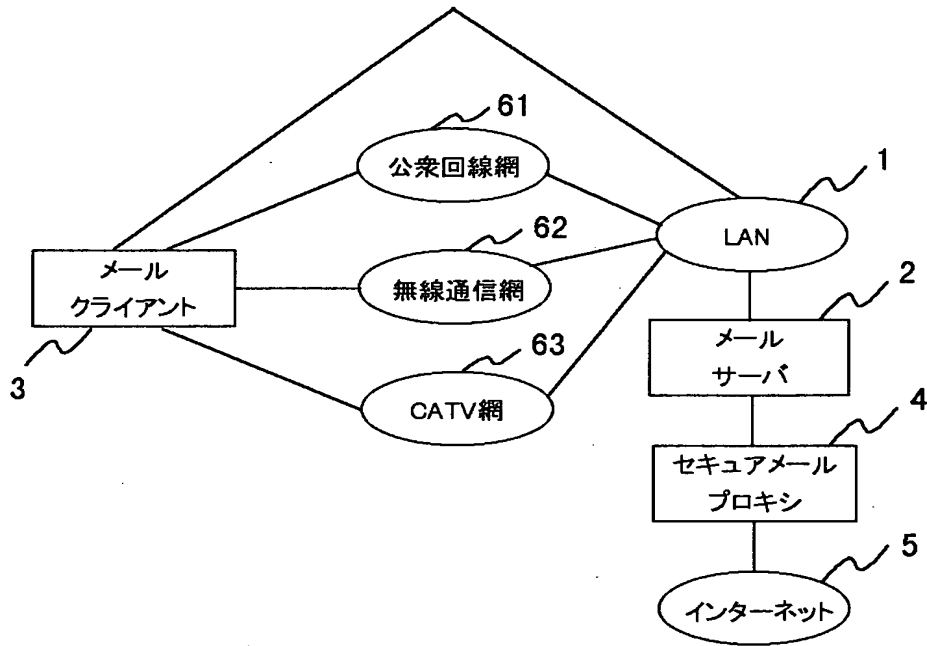
【図 5】

電子メールアドレス	秘密鍵
t-azuma@nec.co.jp	101...001
h-kubota@nec.co.jp	100...100
...	...

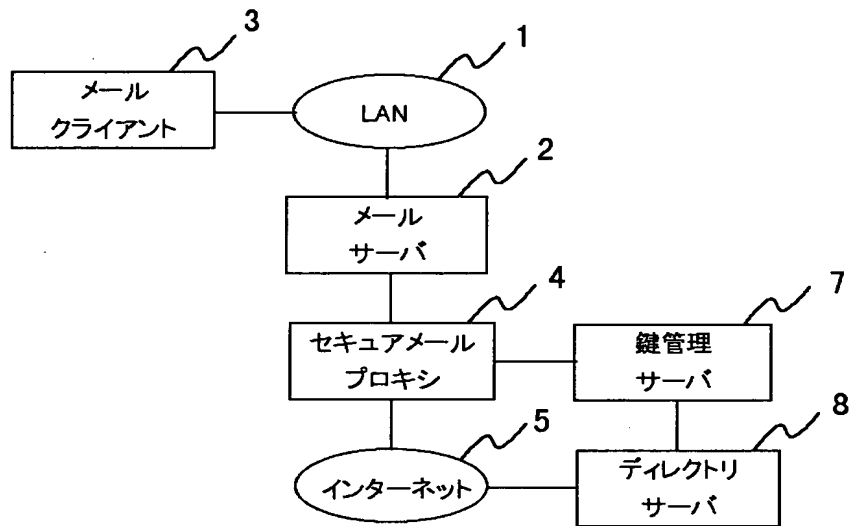
【図 6】

電子メールアドレス	公開鍵
t-azuma@nec.co.jp	110...011
h-kubota@nec.co.jp	101...110
u-suzuki@abc.com	111...001
i-sato@nec.co.us	111...101
...	...

【図7】



【図 8】





【書類名】 要約書

【要約】

【課題】

クライアント側のセキュリティ機能の実装の有無に依存することなく、インターネットにおける電子メールのセキュリティ確保可能とするシステム及び方法の提供。

【解決手段】

L A N 1 上のメールサーバ 2 とインターネット 5 との間にプロキシ 4 を配置し、メールクライアント 3 からの平文メールを受け取ったメールサーバ 2 は L A N 外宛メールは平文のままプロキシ 4 へ送り、プロキシ 4 は平文メールを暗号化し、メール発信者の署名を付けてインターネット 5 へ署名済み暗号化メールを送出し、インターネットから署名済み暗号化メールの改竄の有無をチェックし、メールが改竄されていない場合、暗号化メールを復号化し平文メールとしてメールサーバ 2 へ配送し、メールが改竄されている場合にはメールの受信を拒否し、改竄されたメールが L A N 1 内に入ることを防止する。

【選択図】

図 1

出 願 人 履 歴 情 報

識別番号 [ 0 0 0 0 0 4 2 3 7 ]

1. 変更年月日	1 9 9 0 年 8 月 2 9 日
[ 変更理由 ]	新規登録
住 所	東京都港区芝五丁目 7 番 1 号
氏 名	日本電気株式会社